REMARKS

CLAIMS:

Claims 1-50 comprise the case. Claims 1, 15, 29, and 40 have been amended to state that "said user authentication message" is combined with "at least part of said user identifier" in accordance with the specification, e.g. at page 12, line 4 - page 13, line 4. Applicant respectfully submits that no new matter has been added.

I) 35 U.S.C. 112

Claims 3-5, 17-19, 30-32 and 41-43 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite, in that they depend from Claims 1, 15, 29, and 40 which "implies that" the "user authentication message" be combined with "the entire user identifier", whereas the rejected claims decrypt the "user authentication message by the user decrypting key", which is "part of" the user identifier.

Therefore, Applicant has amended Claims 1, 15, 29, and 40 as discussed above to recite that "said user authentication message" is combined with "at least part of said user identifier". Hence, Applicant respectfully submits that the amendment to Claims 1, 15, 29, and 40 renders Claims 3-5, 17-19, 30-32 and 41-43 definite under 35 U.S.C. 112, second paragraph, and respectfully requests allowance of the claims.

II) 35 U.S.C. 103

A) Claims 1, 6, 8-9, 15, 20, 22-23, 29, 33, 35, 40, 44 and 46:

Claims 1, 6, 8-9, 15, 20, 22-23, 29, 33, 35, 40, 44 and 46 have been rejected as being unpatentable over Anderl et al. (Int. Publication WO 87/07062) in view of Smith (U.S. Patent No. 4,956,769) under 35 U.S.C. 103(a).

1) Claims 1, 15, 29 and 40:

Independent Claims 1, 15, 29 and 40 are separately rejected on similar grounds, the Examiner reciting Anderl et al. in much the same manner as in the immediately preceding Office Action, with the exception that the Examiner now apparently agrees with the arguments by Applicant and the statements by Declarant in sections I and II of the Second Declaration under Rule 1.132.

The Examiner states, e.g. re Claim 1, "Anderl et al. does not teach the computer processor having a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity the user is authorized to conduct with respect to the data storage media, the user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user; and combining the user authentication message with the user identifier from the user table in accordance with the predetermined algorithm to authorize or deny the user activity."

The Examiner relies on Smith to provide these elements, the Examiner stating that "it would have been obvious" to have modified Anderl et al. in accordance with the teachings of Smith.

Applicant respectfully submits that Smith, as pointed out by the accompanying Third Declaration under Rule 1.132, "Smith fails to provide user authentication, relying instead on the normal

fixed installation logon process 'at least one system user, identified by a 'userid' or unique user identification symbol, that is accessing the system from at least one terminal location with a terminal address,' ***. 'Specifically, the user access profile table and the terminal location security access table are constructed within the host system environment ***.' *** Thus, Smith has no relationship to the present '899 Application's 'unique user identifier for each authorized user, ***. The user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user.'"

With respect to Anderl et al., in addition to the above discussion, the Second Declaration under Rule 1.132 points out that Anderl et al. "requires that a login specify the level and password as a specific request. *** In contrast, in the present '899 Application, access permissions of the user table are separate from the authentication method." Further, the Third Declaration under Rule 1.132 points out that, in Anderl et al., "'Security for the card is provided by requiring a separate password for gaining access to each of designated levels of interaction between the card and the associated station.' *** 'This password is checked internally by the card algorithmically against the appropriate password at the same login level in the card header.' *** Any authentication (not directly described) appears to be of the 'card' or 'file' and not the 'user' ***. Thus, Anderl et al. access security is provided by an entirely different mechanism than the present '899 Application's 'unique user identifier for each authorized user, ***. The user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user.'"

Therefore, Applicant respectfully submits that both Smith and Anderl et al. teach away from Applicant's invention, e.g. Claim 1, "A portable security system for managing access ***, said portable security system comprising: a wireless interface ***; and a computer processor *** having a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media, said user identifier, when combined with a user authentication message from said authorized user in accordance with a predetermined algorithm, authorizes said user; said computer processor receiving said user authentication messages from said data storage drive via said wireless interface, combining said user authentication message with at least part of said user identifier from said user table in accordance with said predetermined algorithm to authorize or deny said user activity, and transmitting said user authorization or denial to said data storage drive via said wireless interface."

Applicant thus respectfully requests allowance of independent Claims 1, 15, 29 and 40 under 35 U.S.C. 103(a).

2) Claims 6, 20, 33 and 44:

The Examiner rejected Claims 6, 20, 33 and 44 on Anderl et al. in view of Smith stating that Anderl et al. teaches that the "user table permitted activities comprise a plurality of permitted activities, selected ones of which each of the users may be authorized to conduct, the permitted activities comprising *** 5) add entries to the user table, and 6) change/delete entries to the user table (see Smith ***)."

Applicant respectfully submits that Smith, as pointed out by the accompanying Third Declaration under Rule 1.132, "does not

provide management of access as part of an operational process, nor portability of that management. Rather, Smith discusses 'membership of any one given user can be changed by the security systems programmer at the installation time' for the host system. *** 'Specifically,the user access profile table and the terminal location security access table are constructed within the host system environment ***. After this, each of the respective tables is built ***' ***. Thus, Smith access is established at installation time, and is conducted within the host system, making it non-portable, as opposed to the present '899 Application in which certain users are permitted management of access, and that access is portable. 'The permitted activities in the user table may comprise *** 5) add entries to the user table, and 6) change/delete entries to the user table.'"

With respect to Anderl et al., the Third Declaration under Rule 1.132 points out "Anderl et al. do not provide management of access as part of the operational process, nor portability of that management. Rather, Anderl et al. discuss establishment of access at issuance by the issuer at a particular station. 'The high security header 35 contains information such as *** the passwords for each login level ***. Direct access to the header section is available only to the two top security levels.' *** 'The fourth level of security is that retained by the MASTER ISSUER. It is at this level that the card is formatted and from which it is issued. *** Each account in this example is handled by a separate file on the card and only persons or programs with the proper credentials for a particular file may access that file at an appropriate application station.' *** Thereafter, a password 'can be rewritten by logging into the card at a higher security level ***' ***, but there is no access management."

Therefore, Applicant respectfully submits that both Smith and Anderl et al. teach away from Applicant's invention, e.g. Claim 6, "The portable security system of Claim **1**, wherein said computer processor user table permitted activities comprise a plurality of permitted activities, selected ones of which each of said users may be authorized to conduct, said permitted activities comprising *** 5) add entries to said user table, and 6) change/delete entries to said user table."

Applicant thus respectfully requests allowance of Claims 6, 20, 33 and 44 under 35 U.S.C. 103(a).

3) Claims 8, 22, 35 and 46:

The Examiner rejected Claims 8, 22, 35 and 46 on Anderl et al. in view of Smith stating that Anderl et al. teaches that the "user table comprises a separate entry for each the user identifier, the entry comprising all the permitted activities the user is authorized to conduct (see Smith ***)."

However, the rejected claims each depends from the respective independent claim as discussed above, and the authorization to gain access to the user table is submitted to be patentable over Smith and Anderl et al., as discussed above. Further, Anderl et al. is discussed in the Second Declaration under Rule 1.132 as "a fundamental distinguishing difference exists between the 'designated levels of interaction' of Anderl et al. and the present '899 Application's 'at least one unique user identifier for each authorized user'."

Applicant thus respectfully requests allowance of Claims 8, 22, 35 and 46 under 35 U.S.C. 103(a).

4) Claims 9 and 23:

The Examiner rejected Claims 9 and 23 on Anderl et al. in view of Smith stating that Anderl et al. teaches that the "computer processor additionally comprises a nonvolatile memory storing the user table (see Anderl et al. ***)."

However, the rejected claims each depends from the respective independent claim as discussed above, and the authorization to gain access to the user table is submitted to be patentable over Smith and Anderl et al., as discussed above. Further, Applicant respectfully submits that the "table" of Anderl et al. comprises "passwords for each security level are placed in the card header", and relate to designated levels of interaction between the card and the associated station without regard to the number of actual users at each level, as discussed above.

As pointed out above, in contrast, the "user table" of Claims 9 and 23 is defined as "comprising at least a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct" in respectively Claims 1 and 15, from which Claims 9 and 23 depend.

Thus, Applicant respectfully submits that Claims 9 and 23 patentably define over Anderl et al. and Smith, and Applicant thus respectfully requests allowance of Claims 9 and 23 under 35 U.S.C. 103(a).

B) Claims 2 and 16:

Claims 2 and 16 have been rejected as being unpatentable over Anderl et al. and Smith in further view of Davis (U.S. Patent No. 4,941,201) under 35 U.S.C. 103(a):

The Examiner states that Anderl et al. in view of Smith "does not teach wherein the wireless interface comprises an RF interface." Davis is said to teach "an RF interface". The Examiner further states "it would have been obvious *** to have modified Anderl et al. to include *** an RF interface. *** by the teachings of Davis ***".

Applicant respectfully submits, that as pointed out by the first Declaration under Rule 1.132, Davis "relates to an 'electronic data storage *** apparatus *** wherein a combination power and data signal is received by a preferably portable *** data storage means ***'. *** Davis shows a data storage device with CMOS logic that stores and addresses data, without any user authentication. *** Davis shows an address-like initialization access code to address a particular memory location of the device, but shows nothing directed to a user identifier. *** Davis shows an address-like initialization access code to address a particular memory location of the device, but shows no user authentication or decryption. *** Davis has no ability to manage access."

Applicant therefore respectfully submits that the frequency of the Davis communication signal is not relevant to Applicant's Claims 2 and 16, which depend respectively from Claims 1 and 15, and which define, e.g. Claim 1, "said computer processor receiving said user authentication messages from said data storage drive via said wireless interface, combining said user authentication message with at least part of said user identifier from said user table in accordance with said predetermined algorithm to authorize or deny said user activity, and transmitting said user authorization or denial to said data storage drive via said wireless interface."

Further, Davis is submitted to be unable to make up for the failings of Anderl et al. and Smith as discussed above.

Hence, Applicant respectfully submits that Applicant's Claims 2 and 16 are therefore patentable over Anderl et al., Smith and Davis under 35 U.S.C. 103(a), and respectively requests allowance thereof.

C) Claims 3-5, 17-19, 30-31 and 41-43:

The Examiner rejected Claims 3-5, 17-19, 30-31 and 41-43 under 35 U.S.C. 103(a) as being unpatentable over Anderl et al. and Smith in further view of Wright et al. (U.S. Patent No. 6,084,969).

1) Claims 3, 17, 30 and 41:

With respect to Claims 3, 17, 30 and 41, the Examiner states that Anderl et al. in view of Smith "does not teach wherein each the user identifier comprises a user symbol and a user decrypting key, wherein the user authentication message comprises an encrypted user authentication message which may be decrypted by the user decrypting key, and wherein the computer processor conducts the combination by decrypting the user authentication message by the user decrypting key." Wright et al. is said to teach "an encryption system for a two way pager" having the user identifier and encrypted user authentication message as above, and "wherein the computer processor conducts the combination by decrypting the user authentication message by the user decrypting key ***)." The Examiner further states "It would have been obvious *** to have modified Anderl et al. as modified, by the teachings of Wright et al. ***".

However, Claims 3, 17, 30 and 41 depend from independent Claims 1, 15, 29 and 40 with respect to which Anderl et al. and Smith are submitted to teach away from Applicant's invention.

Further, as pointed out by the Third Declaration under Rule 1.132, in Anderl et al., "'Security for the card is provided by requiring a separate password for gaining access to each of designated levels of interaction between the card and the associated station.' *** 'This password is checked internally by the card algorithmically against the appropriate password at the same login level in the card header.' *** Any authentication (not directly described) appears to be of the 'card' or 'file' and not the 'user' ***. Thus, Anderl et al. access security is provided by an entirely different mechanism than the present '899 Application's 'unique user identifier for each authorized user, ***. The user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user.'

"Further, Anderl et al. fail to encrypt the access process. 'In addition, encryption of data as it is provided to the card is also available for those particular sensitive applications.' *** Without encryption of the access process, communication across an Anderl et al. interface, including the password itself, is in the open.

"Thus, Anderl et al. is further distinguished from the present '899 Application, 'wherein the user authentication message comprises an encrypted user authentication message which may be decrypted by the user decrypting key, ***.

With respect to Smith, the Third Declaration under Rule 1.132 points out "Smith fails to provide user authentication ***.

"Thus, Smith has no relationship to the present '899 Application's 'unique user identifier for each authorized user, ***. The user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user.'

"Further, Smith fails to provide encryption, thus further distinguishing Smith from the present '899 Application, 'wherein

the user authentication message comprises an encrypted user authentication message which may be decrypted by the user decrypting key, ***.

Still further, Applicant points out that Wright et al. is directed to communication of a pager, and does not have a user table, e.g. Claim 1, of "a computer processor mounted in said portable data storage cartridge". Rather, the pager has a single set of keys representing the pager and not separate users (column 7, lines 1-15), and communicates with a central "pager proxy server" (column 4, line 63 - column 5, line 25).

Hence, Applicant respectfully submits that Anderl et al., Smith and Wright et al. teach away from Applicant's use of encryption/decryption with the authorization process, and that therefore Applicant's Claims 3, 17, 30 and 41 are patentable over Anderl et al. in view of Smith and in further view of Wright et al. under 35 U.S.C. 103(a). Applicant therefore respectfully requests allowance of Claims 3, 17, 30 and 41.

2) Claims 4, 18, 31 and 42:

With respect to Claims 4, 18, 31 and 42, the Examiner states that Anderl et al. in view of Smith and in further view of Wright et al. "teaches wherein the user decrypting key comprises a sender public key, and wherein the predetermined algorithm comprises a public key cryptographic algorithm ***."

However, Claims 4, 18, 31 and 42 depend from Claims 3, 17, 30 and 41, wherein Anderl et al., Smith and Wright et al. are submitted to teach away from Applicant's use of encryption/decryption with the authorization process, which is submitted to not be overcome by the particular keys employed by Wright et al. in the communication process.

Therefore, Applicant respectfully submits that Claims 4, 18, 31 and 42 are patentable over Anderl et al. in view of Smith and in further view of Wright et al. under 35 U.S.C. 103(a). Applicant therefore respectfully requests allowance of Claims 4, 18, 31 and 42.

3) Claims 5, 19, 32 and 43:

Claims 5 and 19, and Claims 32 and 43 are rejected separately and in similar fashion. The Examiner states that Anderl et al. in view of Smith and in further view of Wright et al. "teaches wherein the user authentication message is encrypted by a sender private key and a receiver public key ***, and wherein the public key cryptographic algorithm decrypts the user authentication message employing a receiver private key and the sender public key ***."

However, Claims 5, 19, 32 and 43 depend from Claims 4, 18, 31 and 42, wherein Anderl et al., Smith and Wright et al. are submitted to teach away from Applicant's use of encryption/decryption with the authorization process, which is submitted to not be overcome by the particular keys employed by Wright et al. in the communication process.

Therefore, Applicant respectfully submits that Claims 5, 19, 32 and 43 are patentable over Anderl et al. in view of Smith and in further view of Wright et al. under 35 U.S.C. 103(a). Applicant therefore respectfully requests allowance of Claims 5, 19, 32 and 43.

D) Claims 7, 10-13, 21, 24-27, 34, 36-38, 45 and 47-49:

Claims 7, 10-13, 21, 24-27, 34, 36-38, 45 and 47-49 have been rejected as being unpatentable over Anderl et al. in view of Smith, and further in view of Bapat et al. (U.S. Patent No. 6,038,563) under 35 U.S.C. 103(a).

1) Claims 7, 21, 34 and 45:

The Examiner states that, as to Claims 7, 21 and 45, Anderl et al. as modified by Smith does not teach a "user table comprises a separate entry for each the user identifier and the permitted activity the user is authorized to conduct", which is said to be taught by Bapat et al., and it "would have been obvious *** to have modified Anderl et al. as modified, by the teachings of Bapat et al. ***." Claim 34 is similarly rejected.

Bapat et al. relates to a computer network, and shows an "access control database has access control objects that collectively store information that specifies access rights by users to specified sets of the managed objects. The specified access rights include access rights to obtain management information from the network." (column 3, lines 17-21). "An access control procedure limits access to the management information stored in the database tables using at least one permissions table." (column 3, lines 32-35) (emphasis added). "Each 'rule' in the access control tree either grants or denies access by certain groups of users *** to a set of target objects". (column 11, lines 4-6).

However, no "user" has access to the "permissions table" to, e.g., Claim 6, "3) read the user entry of said user table, 4) read all entries of said user table, 5) add entries to said user table, and 6) change/delete entries to said user table".

Rather, in Bapat et al., a "database access engine *** using the permissions table such that each user is allowed access only to management information in the set of database tables that the user would be allowed by the access control database to access." (column 3, lines 42-46).

Further, Applicant respectfully submits that, as discussed above with respect to Claims 1, 15, 29 or 40, from which Claims 7, 21, 34 and 45 depend, and as pointed out by the accompanying Third Declaration under Rule 1.132, as discussed above, "Smith fails to provide user authentication, relying instead on the normal fixed installation logon process". As pointed out by the Second Declaration under Rule 1.132, Anderl et al. fails to show a user identifier that is used in the authentication. Rather, Anderl et al. has a password authentication.

Per the Second Declaration under Rule 1.132, "In contrast, in the present '899 Application, access permissions of the user table are separate from the authentication method. The user table comprises 'at least one unique user identifier for each authorized user, *** and at least one permitted activity the user is authorized to conduct with respect to the data storage media. The user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user.' ***."

Bapat et al. provides a "database access engine *** using the permissions table such that each user is allowed access only to management information in the set of database tables that the user would be allowed by the access control database to access." (column 3, lines 42-46), and does not provide a user identifier for authentication, e.g. of Claim 1, "a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media, said user identifier, when combined with a user authentication message from said authorized user in accordance with a predetermined algorithm, authorizes said user".

Applicant therefore respectfully submits that Claims 7, 21, 34 and 45 are patentable over Anderl et al. as modified by Smith and as modified by Bapat et al. under 35 U.S.C. 103(a), and Applicant respectfully requests allowance thereof.

2) Claims 10, 24, 36 and 47:

With respect to Claims 10, 24, 36 and 47, the Examiner states that Anderl et al. as modified by Smith does not teach "a class table", but that Bapat et al. does teach a "class table comprising at least a unique class identifier for each authorized class of users ***, when combined with a user authentication message from a user of the authorized class of users ***, authorizes the user ***", and that it "would have been obvious *** to have modified Anderl et al. by the teachings of Bapat et al."

Again, as discussed above, Applicant respectfully submits that, with respect to Claims 1, 15, 29 or 40, from which Claims 10, 24, 36 and 47 depend, Anderl et al. as modified by Smith fails to show a user identifier that is used in the authentication. Rather, Anderl et al. has a password authentication. Smith fails to provide user authentication.

Bapat et al. provides a "database access engine *** using the permissions table such that each user is allowed access only to management information in the set of database tables that the user would be allowed by the access control database to access." (column 3, lines 42-46), and does not provide a user identifier for authentication, e.g. of Claim 1, "a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media, said user identifier, when combined with a user

authentication message from said authorized user in accordance with a predetermined algorithm, authorizes said user".

Applicant therefore respectfully submits that Claims 10, 24, 36 and 47 are patentable over Anderl et al. as modified by Smith and as modified by Bapat et al. under 35 U.S.C. 103(a), and respectfully requests allowance thereof.

3) Claims 11, 25, 37 and 48:

With respect to Claims 11, 25, 37 and 48, the Examiner states that Anderl et al. as modified by Smith and as modified by Bapat et al. teaches that the "user table additionally comprises any class membership of each the user".

Again, as discussed above, Applicant respectfully submits that, with respect to Claims 1, 15, 29 or 40, from which Claims 11, 25, 37 and 48 depend, Anderl et al. fails to show a user identifier that is used in the authentication. Rather, Anderl et al. has a password authentication. Smith fails to provide user authentication.

Bapat et al. provides a "database access engine *** using the permissions table such that each user is allowed access only to management information in the set of database tables that the user would be allowed by the access control database to access." (column 3, lines 42-46), and does not provide a user identifier for authentication, e.g. of Claim 1, "a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media, said user identifier, when combined with a user authentication message from said authorized user in accordance with a predetermined algorithm, authorizes said user".

Applicant therefore respectfully submits that Claims 11, 25, 37 and 48 are patentable over Anderl et al. as modified by Smith and as modified by Bapat et al. under 35 U.S.C. 103(a), and respectfully requests allowance thereof.

4) Claims 12, 26, 38 and 49:

With respect to Claims 12, 26 and 49, the Examiner states that Anderl et al. as modified by Smith and as modified by Bapat et al. teaches that the "user table and the class table permitted activities" include "3) read all entries of the class table, 4) add entries to the class table, and 5) change/delete entries to the class table". Claim 38 is similarly rejected.

Again, as discussed above, Applicant respectfully submits that, with respect to Claims 1, 15, 29 or 40, from which Claims 12, 26, 38 and 49 depend, Anderl et al. fails to show a user identifier that is used in the authentication. Rather, Anderl et al. has a password authentication. Smith fails to provide user authentication. Further, Bapat et al. does not provide a user identifier for authentication, e.g. of Claim 1, "a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media, said user identifier, when combined with a user authentication message from said authorized user in accordance with a predetermined algorithm, authorizes said user".

Additionally, Applicant respectfully submits that, in Bapat et al., as discussed above, the permissions table is used to grant access to a database, and further submits that no "user" has access to the "permissions table", to, e.g., Claim 12, "3) read all entries of said class table, 4) add entries to said class table, and 5) change/delete entries to said class table."

Applicant therefore respectfully submits that Claims 12, 26, 38 and 49 are patentable over Anderl et al. as modified by Smith and as modified by Bapat et al. under 35 U.S.C. 103(a), and respectfully requests allowance thereof.

5) Claims 13 and 27:

With respect to Claims 13 and 27, the Examiner states that Anderl et al. as modified by Smith and as modified by Bapat et al. teaches a "nonvolatile memory storing the user table".

Applicant respectfully submits that the "table" of Anderl et al. comprises "passwords for each security level are placed in the card header", and relate to designated levels of interaction between the card and the associated station without regard to the number of actual users at each level, as discussed above. Further, Bapat et al. "stores a full copy of the access control object tree" (column 7, lines 18-19) but does not provide a user identifier for authentication, e.g. of Claim 1, "a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media, said user identifier, when combined with a user authentication message from said authorized user in accordance with a predetermined algorithm, authorizes said user".

Applicant therefore respectfully submits that Claims 13 and 27, which depend from Claims 1 and 15, are patentable over Anderl et al. as modified by Smith and as modified by Bapat et al. under 35 U.S.C. 103(a).

E) Claims 14, 28, 39 and 50:

The Examiner rejected Claims 14, 28, 39 and 50 under 35 U.S.C. 103(a) as being unpatentable over Anderl et al. and Smith in further view of Hastings et al. (U.S. Patent No. 6,370,629).

The Examiner states that Anderl et al. as modified by Smith "does not teach wherein the data stored in the data storage media is encrypted, and wherein the user authorization for the read access additionally comprises a decryption key for the encryption stored data."

The Examiner states that Hastings et al. teaches "wherein the data stored in the data storage media is encrypted ***, and wherein the user authorization for the read access additionally comprises a decryption key for the encrypted stored data ***."

However, Claims 14, 28, 39 and 50 depend from independent Claims 1, 15, 29 and 40 with respect to which Anderl et al. and Smith are submitted to teach away from Applicant's invention.

Further, Applicant points out that Hastings et al. is directed to restricting use of information to designated geographic regions, and does not have a user table, e.g. Claim 1, of "a computer processor mounted in said portable data storage cartridge". Rather, there are encrypted files with associated file decryption keys (column 4, lines 41-57).

Hence, Applicant respectfully submits that Anderl et al., Smith and Hastings et al. teach away from Applicant's use of encryption/decryption with the authorization process, and that therefore Applicant's Claims 14, 28, 39 and 50 are patentable over Anderl et al. in view of Smith and in further view of Hastings et al. under 35 U.S.C. 103(a). Applicant therefore respectfully requests allowance of Claims 14, 28, 39 and 50.

Additional Art:

The additional reference cited by the Examiner (Naito, U.S. Patent No. 6,477,653) has been examined and as best understood, does not teach or suggest Applicant's claimed invention.

SUMMARY:

Claims 1, 15, 29 and 40 have been amended as discussed above.

Applicant respectfully submits that the present invention distinguishes over the cited patents and respectfully requests that the Examiner allow Applicant's Claims 1-50 under 35 U.S.C. 103.

Respectfully submitted,
P. J. Seger

By: _____
John H. Holcombe, (#20,620)
Attorney for Applicants
From: IBM Corporation
Intellectual Property Law
8987 E. Tanque Verde Rd. #309-374
Tucson, AZ 85749
Telephone: (520) 760-6629

JHH/cw
Attachment: Third Declaration